THE MCDANIEL LAW FIRM, PC
54 Main Street
Hackensack, NJ 07601
(201) 845-3232
(201) 845-3777 (fax)
Attorneys for Plaintiff Baseprotect USA, Inc.

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

BASEPROTECT USA, INC. Plaintiff, v. SWARM 1277D[1], an unincorporated joint enterprise, and JOHN DOES 1-161, such persons being presently unknown participants and members of the joint enterprise, Defendants.	2:11-cv-7289 (SDW)(MCA) **DECLARATION OF DAVID FARRIS**

I, **DAVID FARRIS**, have personal knowledge of the facts stated below and, under penalty of perjury under the laws of the Federal Republic Germany, hereby declare:

1. I am the USA key account manager of Baseprotect GmbH, the parent company of Baseprotect USA, Inc. (collectively "Baseprotect"). I submit this Declaration in support of the application of Baseprotect USA, Inc. for a Preliminary Injunction.

2. I am fully familiar with Baseprotect's operations in the United States and the technology at issue in this lawsuit. This Declaration is based on my personal knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

[1] The alpha-numeric hash file assigned to this unique copy of the copyrighted work is truncated. See Schedule A to the Complaint for the complete hash.

3. Baseprotect USA, Inc. is a New Jersey Corporation with its principal place of business of business at 100 Springfield Avenue, Union, New Jersey 07081. Baseprotect USA: is a wholly-owned subsidiary of Baseprotect GmbH, Ltd., a company organized under the laws of the Republic of Germany.

The Role of Baseprotect

4. Baseprotect is a digital rights enforcement company in the business of protecting the holders of valid copyrights from competition from unlawful distribution of pirated copies of copyrighted works. Baseprotect monitors digital distribution of the copyrighted works of its clients both on peer-to-peer networks and from direct download and streaming web sites. Baseprotect is frequently engaged by copyright holders to protect the value of the copyrighted work from being damaged through distribution of pirated copies.

5. Baseprotect, under contract with copyright holders, identifies infringing activity on the Internet, in particular unlawful distribution of pirated works, and collects evidence that identifies the infringers and the dates and the times of unlawful distribution. This information is often used to assist the copyright holder to pursue infringement actions. Baseprotect principally provides these services to owners of copyrights covering movies, music and computer software.

6. A true and accurate copy of information related to the infringing acts at issue in this case is attached hereto as **Exhibit A**.

Torrent Technology

7. The Internet is a collection of interconnected computers and computer networks that communicate with each other, thereby facilitating the unbridled communication of millions of people worldwide. These communications can include piracy of music and motion pictures. Once a sound or motion picture recording is formatted into a digital copy, that file can be

replicated and distributed over the Internet an unlimited amount of times without significant degradation in picture or sound quality.

8. The unlawful distribution of copyrighted sound recordings and motion pictures often occurs over the Internet occurs via "peer-to-peer" ("P2P") networks. In the instant matter, pirated copies of the "movie Weekend" have been and continue to be distributed and redistributed in violation of the rights of the copyright holder among P2P network users using a Bit Torrent Protocol ("torrent").

9. The torrent protocol creates a network of computers, Internet connections and network equipment that permits the torrent members, regardless of limited uploading and downloading capabilities, to participate in transferring large amounts of data across the torrent network. (This type of P2P network using Bit Torrent technology is called a "torrent" or a "swarm.") Each user in a torrent acts as both a file server and a network node, storing, offering to distribute and distributing content to any user that connects to the torrent.

Operation of a Torrent Network

10. In a torrent, the initial file provider chooses to distribute a file with torrent technology. This initial file is called a "seed." The torrent software assigns the file to be shared a unique alpha-numeric number, known as the "hash," that will be used to identify that particular file to other torrent users and breaks the file into hundreds or thousands smaller files. Other users, known as "peers" can then join the P2P network and connect to the seed file in order to download the work to their own computers.

11. Prior to the introduction of bit torrent technology, a user needed to download the entire file from only one other user and that user had to make the entire file available for downloading. Torrent technology, however, breaks the files into small pieces and allows

simultaneous uploading and downloading of the pieces between and among the torrent users. Thus, the torrent protocol provided a quantum advance in the ability of Internet users to virally distribute digital content across the Internet and to do so with the appearance of anonymity.

12. Any individual that distributes works on a torrent must take several affirmative steps to joint the torrent and begin distribution. First, the individual must install a torrent client, which is a program installed on an individual computer to manage torrent distribution. The user must also locate the torrent, which most often is done through "torrent trackers," web sites that identify and advertise torrents from which content can be downloaded.

13. Each individual that joins the torrent begins to receive pieces of the file from other users while at the same time offering the content that they have downloaded to other members of the torrent. In this manner, each person who joins a torrent by beginning to download content becomes a file server for the torrent network. Each Internet service account in a torrent becomes a provider of network communications to the torrent. Most importantly, the torrent protocol requires that users distribute the content stored on their computer across the torrent network created by torrent software.[2]

14. This piecemeal distribution network of users distributing the same content, in this case a movie, is referred to as a "swarm." The swarm is a *discrete* network that distributes content virally across the Internet. Within hours, a torrent can distribute content to tens or even hundreds of thousands of users because there is no technical limit on the ability of the torrent to expand to encompass new users, new file servers and new points of network communications.

Detection of Illegal File-Sharing

[2] Torrent software will permit "leeches," the name given to torrent members who download but do not offer content to the torrent. A torrent, however, is ineffective if there are insufficient Swarm members offering the file for distribution. The issue, however, is not

15. Because torrents do not require a central server, or other subscription requirement, torrents operate through the actions of "anonymous" users. Torrents and their users can be detected and monitored, however, and conclusive evidence of distribution of a particular work by the torrent and by its individual members/operators is available through monitoring technology. This monitoring technology is the basis of the digital rights enforcement services offered by Baseprotect.

16. Baseprotect begins the process of digital enforcement by identifying the unique copies of the copyrighted work that are being shared on the network according to their unique hash. Baseprotect uses automated Internet crawling technology and manual searches to discover the existence of new hashes and the related swarms sharing the file.

17. In this case, Baseprotect identified a unique copy of the work Weekend with the unique alpha-numeric hash 1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1 that was being distributed by the Defendant torrent network. Once Baseprotect identified the unique file being distributed by the torrent swarm, a complete copy of the work was downloaded and manually inspected to ensure that it is, in fact, the copyrighted work.

18. After the Swarm was identified, Baseprotect's servers then connected to the Swarm to record information about the participants and confirm that they were engaged in distribution of the work. The Swarm participants can be identified by the Internet Protocol ("IP") address assigned to their Internet service account by their Internet Service Provider ("ISP"). Baseprotect confirms that the user of the Internet service account is in fact engaged in unlawful distribution of the work by downloading a portion of the file directly from each of the Swarm participants that it identifies.

---

relevant to this application as each of the individual Doe Defendants are confirmed distributors of the work.

19. During monitoring, Baseprotect's servers are able to collect and record the following information about the Swarm and the individual members: The size of the Swarm (based on the number of connected servers); the date and time of distribution by individual members; the individual IP address from which the distribution occurred; the specific torrent program used by the Swarm member; the identity of the file offered for distribution; the size of the file offered for distribution, the fact that the file was, in fact, available for download, the GUID code (a unique machine-specific code incorporating information about the software used, IP address and network card used to communicate with the network) and, in most cases, the port number used by the computer from which the work was distributed.

20. Baseprotect's data is stored in databases. Baseprotect then identifies the ISP that provided the Internet connection and the city and state associated with the particular IP address. This information can then be used by the ISPs to identify the specific account holders. In addition, Baseprotect and the attorneys engaged to prosecute copyright infringement actions perform extensive manual review of the data to determine the location of the individual Defendants using geo-location databases. The geo-location databases associate physical addresses with a group of IP addresses by city and state. Baseprotect further determined that the Swarm had a physical presence in this judicial district with three communication nodes consisting of a file server, communications equipment and an Internet account from which the pirated copy was distributed.

21. Baseprotect's monitoring services adhere in all material respects to the protocols established by the Motion Picture Association of America (MPAA) and Recording Industry Association of America (RIAA). These protocols are used by these trade associations to reliably detect piracy on torrents.

Defendant's Role in the Unauthorized Distribution

22. Baseprotect's monitoring process conclusively identifies unauthorized distribution. By downloading from each of the individual Defendants' computers, we establish that the work was in fact being distributed from that IP address at the date and time recorded by our servers. The evidence establishes (1) the existence of a pirate copy of the work stored on a computer connected to the Internet at that IP address and (2) that the work was in fact being distributed from the computer connected to the Internet at that IP address.

23. As discussed above, the Defendants, both the Swarm 1277D and Movant, identified at this point only by IP address 67.170.86.147, engaged in the unauthorized distribution of Weekend in direct competition with authorized distributors. Baseprotect identified the individual IP accounts from which the distribution occurred as of the date and time on which distribution was observed. In addition, a portion of the copyrighted work downloaded from that address and other information was recorded about the distributor. It is not possible, however, to determine with accuracy whether the same users continue to distribute the work. This is because the vast majority of Internet service accounts use IP addresses that are dynamically assigned and which are changed by the IP periodically. IP addresses that do not change ("static IPs") are generally only used for commercial accounts. Thus, an individual member of the Swarm may be observed on different occasions distributing the work from different IP addresses and duplicate results are relatively commonplace. As long as the work remains in the member's torrent client and the member's computer is connected to the Internet, unlawful distribution continues.

24. The Swarm identified in **Exhibit A** of the complaint (1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1) is the specific network comprised of

peers on the P2P network, each of which, individually and collectively, are conclusively known to have engaged in the distribution of Weekend.

25. The Doe Defendants identified in **Exhibit B** of the complaint are all known to have participated in and thus operated the Swarms identified in **Exhibit A** of the complaint**.** Thus each perpetuated the unlawful distribution for as long as they were – or are – members of the Swarm and as long as their "always on" cable Internet connection remains connected to the Internet and their computer exposes the work for distribution. (In fact, the website for Bit Torrent, the most popular torrent client, contains a user's manual that encourages users to remain connected to the torrent to offer the file to others after their download is complete.)

The Need for Injunctive Relief

26. The Defendant in this case is, in first instance, the specific Swarm identified by its hash number 1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1, which Baseprotect has identified through its P2P monitoring software, manual inspection and ongoing surveillance. As of the date of this Declaration, the Swarm continues to operate and distribute without authorization the copyrighted work that is the subject of this lawsuit.

27. Baseprotect has further identified the Swarm members who distributed the copyrighted work at the dates and times set forth in **Exhibit B**. At this point, Baseprotect is only able to identify these users by their IP addresses and not their actual identities.

28. Because each Swarm is comprised of its individual members and their computer and communications equipment, there is no single information source from which the identities of Defendants can be secured. A copyright holder seeking to prevent infringement of its work on torrents and bring infringement claims against the distributors can only obtain the true identity of

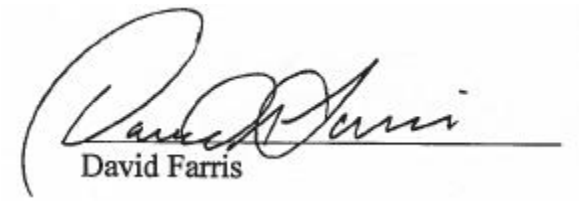
the distributors through the issuance of subpoenas to the ISPs that provided the Internet connection.

29. Without a preliminary injunction, the Swarms and their members will continue to infringe the right of distribution of the copyright holder and to compete with authorized distributors. In order to continue the distribution, they need only turn on the computer and connect to the Internet. Moreover, Baseprotect's experience is also that some owners of Internet service accounts do not password protect their wireless network routers. These open networks can be used by third parties to distribute pirated copies of copyrighted works and unless they are enjoined (and place a password on their wireless network router), the practice will continue.

30. Additionally, ISPs have varying policies concerning the spoliation of their activity logs, as some ISPs erase data faster than. In the event that an activity log is erased, Baseprotect will have no recourse against the infringers whatsoever. A preliminary injunction and expedited discovery order will provide the means by which Baseprotect can notify the ISPs that they are to preserve and produce the true identities of the Internet users identified in **Exhibit B** before activity logs are routinely destroyed.

Under penalties of perjury of the Republic of German, I declare that the foregoing statements made by me are true and correct.

DATED: July 3, 2012



THE MCDANIEL LAW FIRM, PC

EXHIBIT A

John Doe #		ISP	IP Address	Date & Time (UTC)	File Hash	City	State
WKND1277D -	1	BellSouth.net	184.41.198.59	2011.11.17 04:36 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1		
WKND1277D -	2	Charter Communications	75.142.198.23	2011.11.07 09:09 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Riverside	CA
WKND1277D -	3	Comcast Cable	98.253.165.30	2011.11.14 03:39 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	La Grange	IL
WKND1277D -	4	Comcast Cable	76.103.91.195	2011.11.07 01:27 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	San Francisco	CA
WKND1277D -	5	Comcast Cable	71.202.159.206	2011.11.06 10:29 PM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Walnut Creek	CA
WKND1277D -	6	Comcast Cable	24.13.53.79	2011.10.11 03:13 PM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Chicago	IL
WKND1277D -	7	Comcast Cable	68.49.148.50	2011.10.06 07:52 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Lusby	MD
WKND1277D -	8	Comcast Cable	98.243.7.55	2011.11.14 09:48 PM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Detroit	MI
WKND1277D -	9	Comcast Cable	24.19.186.78	2011.11.04 01:24 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Issaquah	WA
WKND1277D -	10	Comcast Cable	67.170.86.147	2011.11.20 09:19 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Seattle	WA
WKND1277D -	11	Cox Communications	72.201.236.172	2011.11.02 02:24 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Mesa	AZ
WKND1277D -	12	Cox Communications	68.0.239.142	2011.11.13 01:18 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Providence	RI
WKND1277D -	13	Frontier Communications	50.46.205.112	2011.10.17 08:34 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Kirkland	WA
WKND1277D -	14	Optimum Online	69.116.237.32	2011.11.19 03:06 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Clifton	NJ
WKND1277D -	15	Optimum Online	24.228.215.170	2011.10.10 06:46 PM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Brooklyn	NY
WKND1277D -	16	Optimum Online	69.112.199.26	2011.10.24 05:33 PM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Brooklyn	NY
WKND1277D -	17	PSINet	38.64.34.50	2011.11.05 04:40 PM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Washington	DC
WKND1277D -	18	Qwest Communications	71.223.10.100	2011.10.17 10:57 PM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Phoenix	AZ
WKND1277D -	19	Road Runner	76.169.145.131	2011.11.09 07:17 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Los Angeles	CA
WKND1277D -	20	Road Runner	75.84.182.137	2011.11.17 09:46 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Van Nuys	CA
WKND1277D -	21	Road Runner	70.124.193.108	2011.10.30 01:24 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Lakeland	FL
WKND1277D -	22	Road Runner	70.124.192.117	2011.11.05 01:58 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Lakeland	FL
WKND1277D -	23	Road Runner	65.190.177.91	2011.11.06 01:11 PM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Holly Springs	NC
WKND1277D -	24	Road Runner	69.203.124.56	2011.11.09 07:16 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	New York	NY
WKND1277D -	25	Road Runner	24.242.19.166	2011.11.12 06:55 PM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	El Paso	TX
WKND1277D -	26	Road Runner	24.167.62.161	2011.11.03 12:30 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Hewitt	TX
WKND1277D -	27	Road Runner	24.167.52.193	2011.10.24 08:50 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Woodway	TX
WKND1277D -	28	SBC Internet Services	99.107.65.34	2011.10.10 06:24 PM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Hollywood	FL
WKND1277D -	29	Verizon Internet Services	98.112.31.26	2011.10.25 02:35 AM	1277D1F87FA9C4F28D43D2C07E9EF6816E366ED1	Victorville	CA